

SAO 91 (Rev. 10/95) Criminal Complaint

UNITED STATES DISTRICT COURT

SEAL BY ORDER
OF THE COURT
UNITED STATES OF AMERICA

NORTHERN DISTRICT OF CALIFORNIA
FILED
FEB 23 PM 2:41

RICHARD H. WICKING
CLERK
U.S. DISTRICT COURT
NO. DIST. OF CA S.J.

MICHAEL A. DALY

(Name of Defendant)

CRIMINAL COMPLAINT

CASE NUMBER:

07 70118 HRL

I, the undersigned complainant, being duly sworn state the following is true and correct to the best of my knowledge and belief. Between in or about July 2003 and February 16, 2007, in the Northern District of California and elsewhere, defendant did, (Track Statutory Language if Offense)

having devised and intended to devise a scheme and artifice to defraud, and for obtaining money and property by means of material false and fraudulent pretenses, representations, and promises, knowingly transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice,

in violation of Title 18, United States Code, §§ 1343 and 2. I further state that I am a Special Agent with the Federal Bureau of Investigation and that this complaint is based on the following facts:

► See Attached Affidavit in Support of Issuance of Criminal Complaint

☒ Continued on the attached sheet and made a part hereof.

Approved as to form:

AUSA Matthew A. Lamberti

Signature of Complainant: Edmund Ewing
Special Agent
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence

February 23, 2007

Date

HON. HOWARD R. LLOYD
United States Magistrate Judge

Name and Title of Judicial Officer

at San Jose, California

City and State

Signature of Judicial Officer

**AFFIDAVIT IN SUPPORT OF ISSUANCE OF
CRIMINAL COMPLAINT**

I, Edmund Ewing, a Special Agent of the Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby declare and state as follows:

A. Introduction and Agent Background

1. I make this affidavit in support of a criminal complaint against Michael A. Daly for mail fraud in violation of Title 18, United States Code, Section 1343. According to his Massachusetts driver's license, number 024443547, Daly was born June 9, 1953 and resides at 18 Lakeview Avenue, Danvers, Massachusetts.

2. The contents of this affidavit are based upon information provided to me by Special Agents of the Federal Bureau of Investigation ("FBI"), witnesses, financial institutions, internet service providers; data obtained from a court-authorized mobile tracking device; as well as my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of supporting a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that Daly committed violations of Title 18, United States Code, Sections 1343 (Wire Fraud) and 2 (Aiding and Abetting the Foregoing Offense).

3. I am a Special Agent with the FBI in the San Francisco Division and have been so employed since February 17, 2006. In that capacity, I have been assigned to investigate federal violations relating to white collar crime. My training includes six months of California Peace Officer Standards and Training ("P.O.S.T.") at San Diego, California, four months of FBI Academy Training at Quantico, Virginia, and Financial and Securities Fraud Specialized

Training in San Francisco, California. As a Special Agent of the FBI, I am authorized to investigate crimes involving fraud and money laundering and have participated in a number of criminal investigations of such crimes.

B. Relevant Statutes

Wire Fraud

4. United States Code, Section 1343 provides in pertinent part:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation affects a financial institution, such person shall be fined not more than \$1,000,000 or imprisoned not more than 30 years, or both

Aiding and Abetting

5. United States Code, Section 2 provides in pertinent part:

Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.

C. Summary of Probable Cause

6. As set forth in more detail below, FBI agents have found that, beginning approximately in July 2003, Daly has engaged in an ongoing scheme to defraud Cisco in which he contacts Cisco using numerous false identities and rented mailboxes around the country, falsely claim malfunctions in Cisco parts under Cisco's SMARTnet warranty program, fraudulently arrange for Cisco to send them replacement parts, sell those parts, and spend at least some of the illegal proceeds on classic automobiles. Daly either does not return any defective parts to Cisco, or return parts not covered by SMARTnet that are worth little or nothing.

D. Statement of Probable Cause**Cisco Systems, Inc.**

7. Cisco Systems, Inc. ("Cisco") is a corporation based in San Jose, California specializing in providing internet networking hardware and software for business, government, and individuals. Cisco's core development areas are in switching and routing, which enable Cisco customers to communicate through the use of the world wide web.

8. One of the services Cisco offers is called SMARTnet. Among other things, SMARTnet provides customers with technical support, including advance hardware replacement (advance hardware replacement allows customers to obtain replacement parts from Cisco immediately, without having first to return the broken part). To obtain the benefits of SMARTnet for a particular product, the customer enters into a SMARTnet contract with Cisco. Among other things, Cisco agrees to provide advance replacement of any failed/defective equipment specifically covered by the contract and the customer agrees to return the failed/defective equipment to Cisco. Typically, Cisco will provide replacement hardware by the next business day, although additional replacements are available, some as fast as two hours. In contrast, the customer needs to send back the failed/defective equipment within 30 days.

9. To provide technical support and/or advance replacement under SMARTnet contracts, Cisco has a service request ("SR") system that allows customers to contact Cisco and obtain assistance with regard to defective or inoperative parts. A customer can initiate an SR by phone and/or by creating an account on Cisco Connection Online ("CCO"), a web-based customer support application. To do so, the customer creates an account on CCO, obtains a username, and logs in to provide the SMARTnet contract number, serial number on the chassis of the

equipment covered by that SMARTnet contract, and a written explanation of the problem. Cisco receives about 3,300 SRs every day or about 1.2 million SRs a year.

10. Service engineers at the Technical Assistance Center ("TAC") engage in an electronic written dialogue with the customer in an attempt to resolve the issue, following a standardized series of resolution attempts. If this protocol does not resolve the issue, the part is deemed defective, and the service engineer will issue a return material authorization ("RMA") number by which Cisco tracks the advance shipped replacement part. Cisco then ships the replacement part, typically using Federal Express ("FedEx"), along with a preaddressed, prepaid United Parcel Service ("UPS") or FedEx label and package for the defective part to be returned. If the original part is not returned, an asset recovery system contacts the customer to remind him of his obligation. If the part is still not returned, or the asset recovery department is unable to contact the customer, the matter is referred to the Service Abuse Investigation Department at Cisco.

Identified Cases of Fraud

11. Beginning in approximately July of 2003, Cisco Service Abuse Investigator Anthony Barberi began documenting a repeated form of SMARTnet fraud occurring through the CCO. This fraud exhibits a common method of execution: An individual, alleging to have in his possession a faulty Cisco part, contacts Cisco customer support online via the CCO. This individual enters into a dialogue with a Cisco customer support employee regarding the malfunctioning Cisco part. The individual provides a valid SMARTnet contract number as well as the serial number of the chassis of the hardware covered by that contract. During this dialogue, the individual uses specific language that prevents the customer support employee from resolving the individual's alleged malfunction through standard troubleshooting. Because

the customer support employee is unable to resolve the malfunction through troubleshooting, Cisco issues an RMA number for the malfunctioning part and ships the individual a replacement part, along with an empty carton for the individual to return the defective product. Subsequently, the individual conducting the fraud returns no defective part to Cisco or, rarely, a part possessing little or no value and not covered by the SMARTnet contract.

12. As of January 25, 2007, a review of this pattern of fraud reveals that 165 SMARTnet contracts have been used; that 72 of these contracts were resold by a company called Data Resource Group ("DRG"), based in Salisbury, Massachusetts, 86 by Evolving Solutions, Inc., based in Hamel, Minnesota, five by PRISM Innovations, Inc., based in Northfield, Illinois, and two by DNX, Inc. (formerly InterNetwork Experts, Inc.), based in Houston, Texas; that approximately 700 SRs have been opened against these contracts in at least 39 states; that Cisco authorized RMAs for all of these RMAs and sent out appropriate replacement parts; that a "failed/defective" part was returned to Cisco only 11 times for these RMAs and that only one time was the returned part properly covered by the SMARTnet contract (the other ten instances involved parts with little or no value that were not covered by the SMARTnet contract).

13. These SRs exhibited a number of common characteristics:

- Almost all of the SRs are opened on CCO through email.
- A majority of email SRs came from same internet service provider, America Online ("AOL").
- All the SRs provide a contact email address created using a free, web-based email company (e.g., Hotmail, Yahoo, Techemail, and others) rather than the domain of the particular company (e.g., amazon.com). Legitimate SRs typically include a company email address for future contact.
- The individual(s) making the SRs purports to be a representative of a particular company and provides an otherwise valid SMARTnet contract number in the name of that company. However, in every single case this company is fictitious.

- The individual(s) making the SRs provides an address for the fictitious company where Cisco can ship the replacement part. In every case, the address is really a private mailbox at a United Parcel Service ("UPS") or Mail Boxes Etc. ("MBE") store.
- Many of the requests use overlapping contact information, SMARTnet contract numbers, and serial numbers. For example, SRs from two different fictitious companies will provide the same contact address.
- The SRs contain valid SMARTnet contract numbers and serial numbers of a part covered by those contracts. Almost all of these SMARTnet contracts were sold by DEG or Evolving Solutions, both registered resellers of SMARTnet contracts. In addition, each of the contracts covered at most only a few pieces of equipment (a single contract can sometimes cover hundreds of pieces of equipment).
- The SRs only seek replacement parts, rather than troubleshooting or any other form of service provided under SMARTnet.
- The SRs use very similar language that seems intended to eliminate the possibility of any troubleshooting and to convince the Cisco representative to simply send a replacement part. According to Cisco representatives, based on formatting and other clues in the emails, it appears that the individual contacting Cisco may be cutting and pasting text from one SR to another. In addition, a few times, when pressed to conduct additional troubleshooting steps, the individual(s) making the SR terminated the session rather than conduct the additional steps.
- Of the approximately 700 cases following the same fraud pattern, SRs are made on the following 12 products: WS-X4516, WS-X6608-T1, WS-X4148-FX-MT, WS-X4515, WS-X6748-SFP, WS-X6K-S2-MSFC2, WS-X4448-GB-SFP, NPE-31, WS-C3550-12G, WS-C4503, WS-X4516-10GE, and WS-X6748-GE-TX. WS-C4503 is a chassis and WS-C3550-12G is a switch; the other ten parts are cards that slide into slots in a chassis. In addition, according to Cisco, these parts are feature rich and particularly in demand. The list prices for these parts range from around \$995 (WS-C4503) to \$25,000 (WS-X6748-SFP). In particular, the list price for the WS-X4516—which the individual contacting Cisco requests about 40 percent of the time—is around \$16,500.
- The individual(s) making the SRs generally sends back no part but sometimes returns a part of little or no value. When a part is sent back, it is almost always sent from the Boston, Massachusetts area, even though the fictitious company requesting the replacement part generally does not have a Boston-area address.

Sampling of Fraud Cases

14. Conducting further investigation, FBI agents chose a random sample of 20 cases from the cases with the fraud pattern described above. For each of these 20 cases, the customer who was supposed to receive the replacement Cisco part was fictitious and the contact address used by the customer to receive that part was really a UPS or MBE store. Agents then examined account documents for these 20 cases. In every case, the UPS or MBE mailbox used for the fraud was rented by Michael A. Daly using Massachusetts driver's license number 024443547. According to that driver's license, Daly lives at 18 Lakeview Avenue, Danvers, Massachusetts 01923-1259 and his date of birth is 6/9/53. Moreover, in every case Daly paid for the mailbox with a credit card belonging to Michael Daly. Finally, in every case, Daly had instructed UPS/MBE to forward the contents of his mailbox to Data Resources Group, 5c Fanaras Drive, Salisbury, Massachusetts 09152.

Fraud Example

15. To illustrate the specific method of this fraud, one of the twenty sample cases occurred as follows. On May 26, 2006, an individual identifying himself as "Scott James" contacted Cisco's customer support using the CCO system. This individual initiated a service request (SR#603652551) and began an electronic conversation with Cisco customer support employee David Loon. The individual described his allegedly defective Cisco product (Part WS-X6748-GE-TX) and the troubleshooting measures he claimed to have already attempted. Portions of this description matched verbatim with descriptions provided by individuals with different names, organizational affiliations, and geographic locations. Approximately 11 minutes later, Loon informed the individual that a replacement WS-X6748-GE-TX would be

shipped, and requested the individual's mailing address. The individual provided the following address:

Delta Logistics
301 Thelma Drive, Suite 437
Casper, Wyoming 82609

16. Loon issued RMA number 81317983 to the request, and the replacement WS-X6748-GE-TX was shipped to the address provided by the individual. In fact, the supposed address for "Delta Logistics" is really a UPS Store in Casper, Wyoming, and Box 437 was at the time rented by Daly, Massachusetts Drivers License Number 024443547, in the name of "Delta Research." On May 31, 2006, Emily LNU at the UPS Store in Casper, Wyoming received a fax from "Mike Daly (Delta Research and Logistics)" stating, "Please forward my package to the following address." Daly provided the address 5C Fanaras Drive, Salisbury, Massachusetts 01952. The UPS store complied with Daly's instructions and forwarded the package to the address he provided. In fact, 5C Fanaras Drive, Salisbury, Massachusetts, 01952 is the address of Michael Daly's business: Data Resources Group. Cisco never received the supposedly defective WS-X6748-GE-TX.

Michael Daly and Data Resources Group

17. Subsequently, FBI agents did further investigation into Michael A. Daly and DRG. Daly, doing business as DRG, operates an internet-based outlet for discount Cisco products. DRG is physically located at 5C Fanaras Drive, Salisbury, Massachusetts. Michael Daly is listed as the Treasurer, Secretary, and President of DRG. DRG maintains five employees on its payroll.

18. Agents have obtained credit card and bank records for DRG showing multiple transactions on personal credit cards in the name of Michael Daly for payments to UPS and

MBE for mailbox rentals throughout the United States. For example, a charge made on May 31, 2006 to an AT&T Universal Card (Account Number ****130397003351) in the name of Michael A. Daly reflects a transaction with UPS Store number 2200 in Casper, Wyoming for \$143.21. This location and amount match the forwarded package referred to in the example described above.

America Online Account

19. Also present in records agents have reviewed is evidence of payments for multiple AOL accounts. This evidence is significant because, using internet protocol ("IP") addresses and other information, agents traced instances of the SMARTnet fraud described above to the AOL account number 0890179701 and screen name "drgdamian." This account is billed to Daly and registered to Damian Prescott at DRG's business address: 5c Fanaras Drive, Salisbury, Massachusetts. Damian Prescott receives regular payroll checks from DRG and is believed to work for Daly.

20. For example, agents examined two instances of the above-described fraud and found that in both cases the IP address used to access the AOL service account of "drgdamian" at the time of the fraud was 69.164.68.245. The IP address 69.164.68.245 is assigned to Adelphia Communications Corporation ("Adelphia") in Amesbury, Massachusetts. Adelphia, a provider of high-speed cable internet, issued the IP address 69.164.68.245 to DRG at the physical location 5C Fanaras Drive #C, Salisbury, MA 01952-1444.

Additional Evidence of Fraud

21. I believe that, once Daly fraudulently obtains parts from Cisco, he then sells them to companies that sell discounted Cisco products over the internet.

22. A review of DRG's bank records shows that DRG regularly receives and deposits checks from several companies selling discounted Cisco products over the internet, including Evolving Solutions, Inc., NaLogic LLC, Scotchcom LLC and Nova DataCom LLC. For example, on July 7, 2006, DRG cashed a check from Nova Datacom LLC for \$40,500, and on July 19, 2006, DRG cashed a check for \$13,500 from NaLogic and a check for \$12,000 from Nova DataCom. I believe that this information, and other evidence, shows that Daly sells the parts he fraudulently obtains from Cisco.

Confirmation of Fraud Through Use of a Tracking Device

23. On February 6, 2007, United States Magistrate Judge Patricia V. Trumbull signed an order authorizing FBI agents to install and monitor a mobile tracking device embedded inside of a package containing a Cisco card, product number WS-X4516, serial number JAB084203LP.

24. On February 13, 2007, agents installed the device and waited for Daly or one of his associates to make an RMA request under a SMARTNET contract believed to be connected to Daly and DRG.

25. On February 16, 2007, Cisco identified an SR that seemed to come from Daly. In this SR, an individual identifying himself as Peter Buckner contacted Cisco's customer support using the CCO system. This individual initiated a service request (SR #605399701) and began an electronic conversation with Cisco customer support employee Christina Santos. The individual described his allegedly defective Cisco product (Part WS-X4516) and the troubleshooting measures he claimed to have already attempted. Portions of this particular description matched verbatim with earlier descriptions provided by individuals with different names, organizational affiliations, and geographic locations who fraudulently obtained Cisco parts and who are believed to be Daly. Approximately 10 minutes later, Santos informed the individual that a

replacement WS-X4516 would be shipped, and requested the individual's mailing address. The individual provided the following address:

Cardinal Technologies
700 North Colorado Blvd
Unit 310
Denver, CO 80206
Attn Peter Buckner

Santos assigned the RMA number 81679877 to the request, and the same day Cisco shipped "Peter Buckner" the replacement WS-X4516, serial number JAB084203LP, along with the tracking device to the address he provided. Cisco's list price for a WS-X4516 is around \$16,500.

26. Not surprisingly, the address "Peter Buckner" provided for "Cardinal Technologies" is really the address for a UPS Store in Denver, Colorado. Moreover, Unit 310 at the UPS Store is registered to Michael Daly of 5C Fanaras Drive, Salisbury, MA, Massachusetts Driver's license number 0244 43547.

27. On February 19, 2007, through the tracking device, agents confirmed the package was at the Denver, Colorado UPS Store. Moreover, agents determined that records from this store confirm that on February 19, 2007, a package was forwarded from "Cardinal Technologies/Mike Daly/700 N Colorado Blvd/Denver, CO 80206" to "Mike Daly/5C Fanaras Drive/Salisbury, MA 01952-1444," UPS tracking number 1Z10FE310118215972. UPS tracking information shows the package was delivered to a Salisbury, Massachusetts address on February 20, 2007 at 9:58 a.m.

28. On February 21, 2007, through the tracking device, agents confirmed that the package was at 7410 Adams Park Court, Annandale, Virginia. The address 7410 Adams Park Court, Annandale, Virginia corresponds with a business complex with the address 7361

McWhorter Place, Suite 310, Annandale, Virginia. That is the address of NovaDataCom.

NovaDataCom is a business selling used Cisco parts on the internet. Since March 2005, DRG has received 42 payments totaling \$704,250 dollars from NovaDataCom. Based on the shipment of the package from Cisco to a UPS Store in Denver to Daly/DRG to NovaDataCom, and the frequent payments DRG receives from NovaDataCom, I believe that Daly fraudulently obtained a WS-X4516, serial number JAB084203LP, from Cisco and sold it to NovaDataCom.

E. Conclusion

29. Based on the information and evidence contained in this affidavit, I believe that probable cause exists that Michael Daly, doing business as Data Resources Group, 5C Fanaras Drive, Salisbury, Massachusetts, committed wire fraud and aided or abetted wire fraud, in violation of Title 18, United States Code, Sections 1343 (Wire Fraud) and 2 (Aiding and Abetting the Foregoing Offense). Specifically, I believe that probable cause exists that Daly made up and aided or abetted a scheme or plan for obtaining property from Cisco by making false statements; that he knew that those statements were false; that those statements were material, that is, they would reasonably influence a person to part with property; that he acted with the intent to defraud; and that he used or caused to be used the wires to carry out or attempt to carry out an essential part of the scheme.

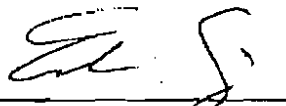
//

//

//

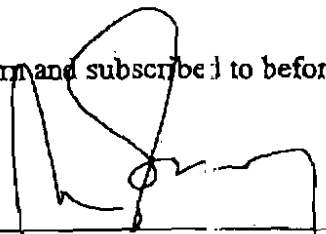
F. Request for Sealing

30. I respectfully request that this complaint and affidavit be sealed until the arrest of the defendant in this case or until such time as the Court directs. Disclosure of the complaint and affidavit at this time could seriously jeopardize the ongoing investigation, as such disclosure would give Daly an opportunity to destroy evidence, notify confederates, or otherwise interfere with the investigation. It may also take some time to locate Daly before his arrest.



EDMUND EWING
Special Agent, FBI

Sworn and subscribed to before me this 23 day of February, 2007



HOWARD R. LLOYD
United States Magistrate Judge

AO 442 (Rev. 5/93) Warrant for Arrest

SEALED BY ORDER
OF THE COURTUnited States District Court
Northern District of California

UNITED STATES OF AMERICA,

v.

MICHAEL A. DALY

RECEIVED
WARRANT FOR ARREST7 FEB 23 P2:55
CASE NUMBER:To: The United States Marshal
and any Authorized United States OfficerNORTHERN DISTRICT
OF CALIFORNIA

07 70118

HRL

YOU ARE HEREBY COMMANDED to arrest MICHAEL A. DALY and bring him or her forthwith to
the nearest magistrate judge to answer a(n)☐ Indictment ☐ Information ☒ Complaint
☐ Order of Court ☐ Violation Notice ☐ Probation Violation Petition

charging him or her with

having devised and intended to devise a scheme and artifice to defraud, and for obtaining money
and property by means of material false and fraudulent pretenses, representations, and promises,
knowingly transmit and cause to be transmitted by means of wire communication in interstate
and foreign commerce writings, signs, signals, pictures, and sounds for the purpose of executing
such scheme and artifice,in violation of Title 18 United States Code, Section(s) 1343Howard R. Lloyd

Name of Issuing Officer

U.S. Magistrate Judge

Title of Issuing Officer

Signature of Issuing Officer

February 23, 2007, San Jose, CA

Date and Location

Bail fixed at \$ No Bailby Howard R. Lloyd
Name of Judicial Officer

RETURN

This warrant was received and executed with the arrest of the above-named defendant at _____

Date received

Name and Title of Arresting Officer

Signature of Arresting Officer

Date of Arrest

SEAL BY ORDER
OF THE COURTUNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISIONORIGINAL
FILED

07 FEB 23 PM 2:41

RICHARD W. WIEKING
CLERK
U.S. DISTRICT COURT
NO. DIST. OF CALIF.

UNITED STATES OF AMERICA,

Plaintiff,

v.

MICHAEL A. DALY,

Defendant.

No.

07 70118 HRL

~~[Proposed]~~ORDER GRANTING MOTION TO
SEALUNDER SEAL

Upon motion of the government, and good cause appearing,

IT IS HEREBY ORDERED that the complaint in this matter (including the affidavit in support of the complaint and accompanying documents) in the above-captioned matter, along with the United States' motion to seal and this order, shall be sealed until the defendant's initial appearance or further order of the Court.

DATED: 2/28/07


HOWARD R. LLOYD
United States Magistrate Judge